Original document

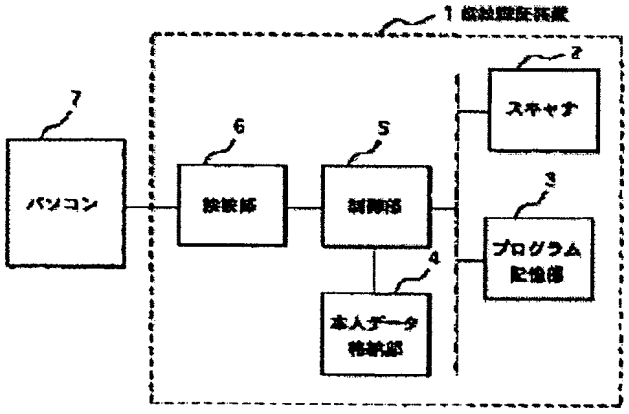
PERSONAL COMPUTER SYSTEM

Publication number: JP2000298529
Publication date: 2000-10-24
Inventor: INABA FUMIO
Applicant: NIPPON ELECTRIC CO
Classification:
- international: ***G06F1/00; G06F12/14; G06F15/00; G06F21/20; G06F21/24; G06T7/00;*** **G06F1/00; G06F12/14; G06F15/00; G06F21/00; G06F21/20; G06T7/00;** (IPC1-7): G06F1/00; G06F15/00; G06T7/00
- European:
Application number: JP19990104409 19990412
Priority number(s): JP19990104409 19990412

View INPADOC patent family
View list of citing documents

Report a data error here

Abstract of **JP2000298529**
PROBLEM TO BE SOLVED: To unnecessitate a CPU and a memory having high performance for a user certification device and to attain the simplification and cost reduction of the certification device while maintaining certification performance by allowing a personal computer(PC) to execute most advanced processing such as image processing, feature extraction and certification which are executed in the certification device hereto fore.
SOLUTION: This system has a PC 7 and a user certification device 1, the PC 7 is provided with a central processing unit (CPU) and a memory at least an the device 1 is provided with a physical information reading means 2 for reading out the information on a user's physical portion, a storage means 3 for storing the feature data of a normal user and a physical information certification program and a control means 5 for controlling the operation of the device 1 and constituted so that the certification program stored in the storage means 3 is inputted to the memory of the PC 7 and executed by using the CPU and the memory built in the PC 7.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－298529
（Ｐ2000－298529Ａ）
(43)公開日　平成12年10月24日(2000.10.24)

(51)Int.Cl.⁷		識別記号	FI		テーマコード*(参考)
Ｇ０６Ｆ	1/00	３７０	Ｃ０６Ｆ	1/00	３７０Ｅ　５Ｂ０４３
	15/00	３３０		15/00	３３０Ｆ　５Ｂ０８５
Ｇ０６Ｔ	7/00			15/62	４６０

審査請求　有　　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願平11－104409

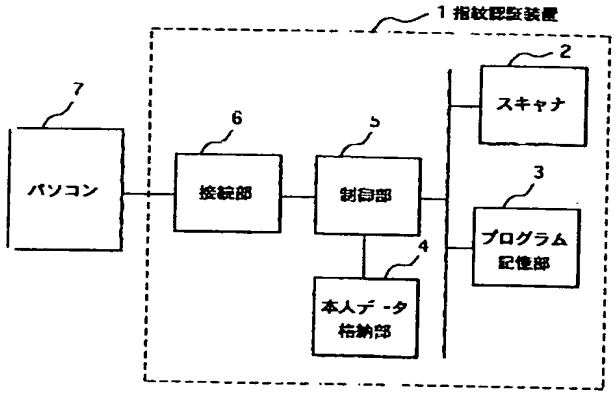
(22)出願日　平成11年４月12日(1999.4.12)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　稲葉　文夫
東京都港区芝５丁目７番１号　日本電気株式会社内
(74)代理人　100096024
弁理士　柏原　三枝子

Ｆターム(参考)　5B043 AA05 AA09 BA02 CA05 FA03 GA01
5B085 AC02 AE23 AE25

(54)【発明の名称】　パーソナルコンピュータシステム

(57)【要約】
【課題】　従来は認証装置内で行っていた画像処理、特徴抽出、認証といった最も高度な処理をパソコン側で担うことにより、ユーザ認証装置には高性能のＣＰＵやメモリを不要として、認証性能を維持しつつ認証装置の簡素化・低コスト化を実現する。
【解決手段】　パーソナルコンピュータとユーザ認証装置とを有し、前記パーソナルコンピュータが少なくとも中央処理装置とメモリとを具えると共に、前記ユーザ認証装置が、ユーザの身体部位の情報を読込む身体情報読取り手段と、正規ユーザの特徴データ及び前記身体情報の認証プログラムを格納した記憶手段と、該装置の動作を制御する制御手段とを具え、前記ユーザ認証装置の記憶手段に格納されている認証プログラムを前記パーソナルコンピュータのメモリに取込んで前記パーソナルコンピュータの中央処理装置及びメモリを用いて実行するようにシステムを構成する。



【特許請求の範囲】
【請求項１】　パーソナルコンピュータとユーザ認証装置とを有するパーソナルコンピュータシステムにおいて、前記パーソナルコンピュータが少なくとも中央処理装置とメモリとを具えると共に、前記ユーザ認証装置が、ユーザの身体部位の情報を読込む身体情報読取り手段と、正規ユーザの特徴データ及び前記身体情報の認証プログラムを格納した記憶手段と、該装置の動作を制御する制御手段とを具えており、前記ユーザ認証装置の記憶手段に格納されている認証プログラムを前記パーソナルコンピュータのメモリに取込んで前記パーソナルコンピュータの中央処理装置及びメモリを用いて実行することを特徴とするパーソナルコンピュータシステム。
【請求項２】　請求項１に記載のパーソナルコンピュータシステムにおいて、前記照合プログラムは、少なくとも、前記ユーザ認証装置の身体情報読取り手段で得た身体情報のデータ処理を行う工程と、この処理により得たデータから特徴抽出を行う工程と、ここで得た特徴データと前記ユーザ認証装置の記憶手段に格納されている正規ユーザの特徴データとを照合する工程と、を実行することを特徴とするパーソナルコンピュータシステム。
【請求項３】　請求項１又は２に記載のパーソナルコンピュータシステムにおいて、前記認証プログラムをパーソナルコンピュータに取込み実行する工程は、前記システムの電源投入時であって前記パーソナルコンピュータのオペレーティングシステムの起動前に行うことを特徴とするパーソナルコンピュータシステム。
【請求項４】　請求項３に記載のパーソナルコンピュータシステムにおいて、前記認証プログラムの照合により特徴データが一致した場合に、前記オペレーティングシステムの起動に際して前記パーソナルコンピュータのメモリにおける前記認証プログラムに関するデータを消去することを特徴とするパーソナルコンピュータシステム。
【請求項５】　請求項１乃至４に記載のパーソナルコンピュータシステムにおいて、前記パーソナルコンピュータとユーザ認証装置とはユニバーサルシリアルバス（ＵＳＢ）インターフェースで接続していることを特徴とするパーソナルコンピュータシステム。
【請求項６】　請求項１乃至５に記載のパーソナルコンピュータシステムにおいて、前記ユーザ認証装置が指紋認証装置であり、前記身体情報読取り手段が指紋の画像を読込むスキャナであることを特徴とするパーソナルコンピュータシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はパーソナルコンピュータ（以下、適宜パソコンあるいはＰＣとも称す。）システムに関し、特に、システムの起動時に身体情報を用いて正規ユーザか否かの照合を行うことによりセキュリティ性を向上させたパーソナルコンピュータシステムに関する。
【０００２】
【従来の技術】コンピュータシステムにおいては、種々のユーザ認証手段を用いて正規ユーザのみシステムにログオン可能にして、セキュリティを確保するようにしている。このユーザ認証手段としてはパスワード方式やＩＤカード方式が広く用いられているが、パスワード方式ではパスワードをユーザが忘れたりパスワードが第三者に流出するという問題があり、ＩＤカード方式でもカードの盗難によるシステム侵入といった問題があった。そこで、近年では、個人毎に独特なパターンを有する指紋や声紋等の身体情報を読取り、予め登録された正規ユーザのものと照合することによりユーザの認証を行うシステムが開発されている。このように身体情報を用いてユーザ認証を行うことにより、パスワードの漏洩やＩＤカードの盗難等によるシステムへの侵入といった問題が解消された。
【０００３】この種のユーザ認証方式を用いたシステムは、パソコンに例えば指紋認証装置を接続して指紋認証を用いた本人認証を行い、本人以外ではそのパソコンが正常に起動しないようにしている。図５は、従来の指紋認証装置の構成を示すブロック図である。従来の指紋認証装置４０は、指紋画像を読取るスキャナ４１と、この画像を処理する画像処理部４２と、個人ごとに異なっている特徴を抽出する特徴抽出部４３と、予め正規ユーザの特徴データを記憶させた格納部４５と、装置１０を制御し読取った指紋の特徴データと正規ユーザの特徴データとの照合を行う制御部４５（ＣＰＵ）と、パソコンと接続するための接続部４６とで構成されている。
【０００４】このシステムの電源投入時にはユーザに指紋押捺リクエストが出され、これに応じてユーザが指紋スキャナ部４１に指を押しつけることにより、指紋画像データが得られる。ここで得た指紋画像データは画像処理部４２、特徴抽出部４３の処理を経て、指紋の特徴データが抽出される。制御部４５よりこの特徴データと予め格納部４４に格納されている正規ユーザの特徴データとの照合が行われ、その結果が接続部４６からパソコン４７へ通知される。この通知によりパソコン４７が正規ユーザを確認できた場合に初めてパソコン４７へのアクセスが許可される。
【０００５】また、特開平９－３３０１４０号公報には、パソコンに一体的に指紋認証機能を組込んだパーソナルコンピュータ装置が開示されている。この装置ではパソコンのキーボードに指紋読取り部が設けられており、ここにオペレータが操作時に指を押しつけるとパソコン本体の指紋照合部にて登録済みの指紋データと照合され、一致した場合にログインが許可される。
【０００６】
【発明が解決しようとする課題】しかしながら、図４に

示す従来の指紋認証装置は、認証装置側で正規ユーザか否かの認証処理を全て行い、その結果のみをパソコン４７に通知するよう構成されている。すなわち、この指紋認証装置は少なくとも、指紋スキャナと、画像処理部と、特徴抽出部と、本人データ格納部と、制御部としての高性能ＣＰＵと、接続部とを具備する、インテリジェント型と呼ばれる比較的高機能なものである必要がある。従って、使用に耐えうる程度の機能を持たせようとすると、この認証装置の製造コストは高いものとなり、かつ装置の小型化にも限界があるという問題を有する。

【０００７】一方、特開平９－３３０１４０号公報の記載にあるような指紋認証機能がパソコンに組込まれているタイプのパーソナルコンピュータ装置では、指紋の照合はパソコン本体で行い、正規ユーザの指紋データもパソコン本体の記憶手段に格納されている。従ってパソコンの強大なＣＰＵやメモリを使用して指紋認証を行うことができるが、これらの動作の制御を行うにはパソコンがオペレーティングシステム（ＯＳ）下で通常動作している環境が必須である。

【０００８】パソコンの電源投入後にはまずＢＩＯＳ（Basic Input/Output System）が動作し、その後ＯＳが起動する。電源投入からＯＳが起動するまでは暫く時間がかかるため、その後に指紋の認証を行うのは例えば認証不一致となった場合等に不経済なものとなる。また、認証プログラムは規模が大きく多くのリソースを必要とするため、この点でも更に規模の大きなＯＳが起動する前に認証を行うことが望ましいといえる。そのためにはＢＩＯＳエリアに認証用プログラムを格納しておく必要があるが、通常ＢＩＯＳは１ＭＢ以内の限られたエリアに格納されるため、ここに大きな認証プログラムを収容しておくのは困難であった。

【０００９】本発明はこのような事情を鑑みてなされたものであり、パーソナルコンピュータシステムにおいて、システムの電源投入後であってパソコンのＯＳ起動前に本人か否かの認証を行い、かつ、パソコンに接続される認証装置の機能を省略して構成を簡単化し、製造コストを低減させたシステムを提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するために、本発明のシステムは、パーソナルコンピュータとユーザ認証装置とを有するパーソナルコンピュータシステムにおいて、前記パーソナルコンピュータが少なくとも中央処理装置とメモリとを具えると共に、前記ユーザ認証装置が、ユーザの身体部位の情報を読込む身体情報読取り手段と、正規ユーザの特徴データ及び前記身体情報の認証プログラムを格納した記憶手段と、該装置の動作を制御する制御手段とを具えており、前記ユーザ認証装置の記憶手段に格納されている認証プログラムを前記パーソナルコンピュータのメモリに取込んで前記パーソナルコンピュータの中央処理装置及びメモリを用いて実行することを特徴とする。

【００１１】このように、本発明では、パソコンと別体として接続されるユーザ認証装置に画像処理、特徴抽出、認証の各プログラムを格納しておき、パソコンのＯＳが起動する前にこの認証プログラムと本人の指紋データをパソコン側に読出し、ＯＳがまだ使用していない状態のパソコンのメモリとＣＰＵを用いて指紋の認証を行うようにしている。従って、従来は認証装置内で行っていた画像処理、特徴抽出、認証といった最も高度かつ複雑な処理をパソコン側で担うようにしたため、ユーザ認証装置には高性能のＣＰＵやメモリを不要とし、認証装置の簡素化・低コスト化を実現することができる。同時に、パソコン側の強大なＣＰＵ及びメモリを用いてユーザ認証を行うようにしているため、パソコンに認証機能を組込んだ一体型のシステムに劣らない性能で認証を行うことができる。

【００１２】また、本発明のパーソナルコンピュータシステムでは、前記認証プログラムをパーソナルコンピュータに取込み実行する工程は、前記システムの電源投入時であって前記パーソナルコンピュータのオペレーティングシステムの起動前に行うことを特徴とする。このようにパソコンのＢＩＯＳ動作時に認証装置からプログラム及びデータをロードして認証を行うようにすれば、ＢＩＯＳ内に認証プログラムを収容しなくてもＯＳ起動前にユーザ認証を経済的かつ簡単に行うことができる。

【００１３】

【発明の実施の形態】本発明の実施の形態を、添付の図面を参照しながら以下に説明する。図１は本発明に係るパーソナルコンピュータシステムの構成を示すブロック図である。図１に示すように、本実施形態に係る指紋認証装置１は、指紋スキャナ２と、プログラム記憶部３と、本人データ格納部４と、制御部５と、ＵＳＢ（Universal Serial Bus）接続部６とを具えており、このＵＳＢ接続部６を介してパソコン７と接続されている。

【００１４】プログラム記憶部３には、指紋スキャナ２で読込んだ画像データについて画像処理、特徴抽出、照合処理を実行する認証プログラムが格納されている。システムの電源投入時には、制御部５の制御により、プログラム記憶部３にある認証プログラムと、スキャナ２で読込んだ画像データと、格納部４に格納されている本人データとが、パソコン７に送られる。

【００１５】図２は、図１に示すパソコン７の構成を示すブロック図である。図２に示すように、パソコン７は、前記指紋認証装置１と接続するＵＳＢ接続部２１と、ＢＩＯＳ２２と、メモリ２３と、高性能ＣＰＵ２４と、ＯＳが格納されているＨＤＤ（ハードディスクドライブ）２５とを具えている。このパソコン７には一般的なパーソナルコンピュータを用いることができ、図２では本発明の理解に必要な最小限の要素しか図示しない

が、モニタやキーボード等の必要な構成要素を具えるものとし、また様々な周辺機器やネットワークと接続していても良い。

【００１６】図３は、本実施形態に係るＰＣシステムの動作を説明するフローチャートである。図３において左側には指紋認証装置１の動作を示し、右側にはパソコン７の動作を示す。このシステムの電源が投入されると（ステップＳ１）、パソコン７ではＢＩＯＳが動作し、認証装置１のプログラム格納部３から認証プログラムがパソコン７に転送される（ステップＳＡ１）。この認証プログラムはパソコン７のメモリ２３に格納され（ステップＳＢ１）、パソコン７のＣＰＵ２４及びメモリ２３を使用して実行される（ステップＳＢ２）。

【００１７】パソコン７にて認証プログラムが実行されると、パソコン７のモニタから又は指紋認証装置１にてユーザに指紋押捺リクエストが出され、これに応じてユーザがスキャナ２に指を押し当てると、得られた指紋画像がパソコン７に送られる（ステップＳＡ２）。この指紋画像に対してパソコン７のリソースを使用して画像処理・特徴抽出が行われ、読込み指紋画像の特徴データが得られる（ステップＳＢ３）。

【００１８】更に、指紋認証装置１の本人データ格納部４から、予め登録してある正規ユーザの特徴データがパソコン７に転送される（ステップＳＡ３）。パソコン７では、読込み指紋画像の特徴データと転送された本人データとの照合が行われる（ステップＳＢ４）。この比較照合において両データが一致した場合には（ステップＳＢ５）、ＯＳに引渡すためにメモリ２３の内容が消去され（ステップＳＢ７）、ＨＤＤ２５に格納してあるＯＳの起動指示が出される。一方、ステップＳＢ５の照合においてデータ不一致となった場合は、正規ユーザ以外の不正アクセスとみなし、ＯＳの起動が拒否される（ステップＳＢ８）。

【００１９】図４は、パソコン７のメモリ２３の一例を示す図である。図４に示すように、パソコン７に実装されたメモリ空間２３は、前記指紋認証装置１から受取った認証プログラム、読込み指紋データ、及び本人特徴データの格納部３２と、認証プログラムの実行すなわち画像処理・特徴抽出・照合処理といった指紋認証のために使用されるワークエリア３３と、ＢＩＯＳ　ＲＯＭ空間３４とを具える。一般にパソコンのＢＩＯＳは１ＭＢ以下の限られた空間３４の一部に格納されており、容量に限りがあるため例えば指紋認証プログラム等の大きなプログラムを実装することは困難である。そこで本発明では認証プログラムは外部装置である指紋認証装置１に格納しておき、システム電源投入時にパソコン側のメモリ２３に取込むことで、ＢＩＯＳ動作時の認証プログラム実行を実現している。なお、上述したように、パソコン７にロードされた認証プログラムは、ＯＳが起動していない未使用メモリ空間で動作して、正規ユーザである認証結果を得た後はＯＳに引渡すために消去されるため、その後のＯＳ起動に影響を及ぼすことはない。

【００２０】図１に示すように、本発明の指紋認証装置１は図４に示す従来の装置に比べて画像処理部４２と特徴抽出部４３を有さず、また制御部５は読込み指紋データと本人データとの照合作業は行わない。上述の通り認証プログラムをパソコン７で動作させることにより、従来は指紋認証装置側で従来行っていた画像処理、特徴抽出、特徴データの照合といった一連の作業を行う必要がなく、制御部５はシステム電源投入時に認証プログラム、スキャナ取込み画像、本人特徴データをパソコン７に送付するだけで良い。この作業は比較的機能の低いＣＰＵで容易に達成することができるため、指紋認証装置に高性能ＣＰＵを設けることなくノンインテリジェント型として低コスト化・製造容易化を図ることができる。

【００２１】以上、本発明の一実施形態について詳細に説明したが、本発明の技術的範囲は上記実施形態のものに限るものではなく、他にも様々な形態として具現することができる。特に、上記実施形態では指紋認証により正規ユーザか否かの判別を行うようにしているが、個人毎にパターンの異なる身体部位であれば指紋に限ることなく、例えば声紋や眼球の網膜パターンを用いて認証を行うようにしても良い。これらの変化は周知技術の転用によって当業者であれば容易に行うことができる。また、上記実施形態では認証装置とパソコンとの接続にＵＳＢインターフェースを用いているが、他のインターフェースを用いても良い。更に、パソコン７はデスクトップ型あるいはラップトップ型に限定されず、そのＯＳやスペック、あるいは認証装置のスキャナの種類も限定されるものではない。

【００２２】

【発明の効果】上記に詳細に説明したように、本発明のシステムでは、読込んだ指紋画像についての画像処理、特徴抽出、及び登録されている本人データとの照合を実行し、データが一致した場合のみＯＳの起動を許可する指紋認証プログラムをＯＳの起動前のＢＩＯＳ動作段階でパソコンに転送し、パソコン側の未使用のメモリ空間及び強大なＣＰＵを使用してこれらの動作を行うようにしているため、従来の指紋認証装置が行っていた動作を省略している。これにより、指紋認証装置側の機能を省略することができ、製造コストの低減及び装置の装置の小型化を実現することができる。

【００２３】また、パソコン７にてＯＳ起動前に強大なＣＰＵと未使用のメモリ空間を使用して認証プログラムを動作させるようにしているため、ＯＳ起動後に認証プログラムを動作させる従来のシステムに比して認証作業を迅速に行うことができる。

【図面の簡単な説明】

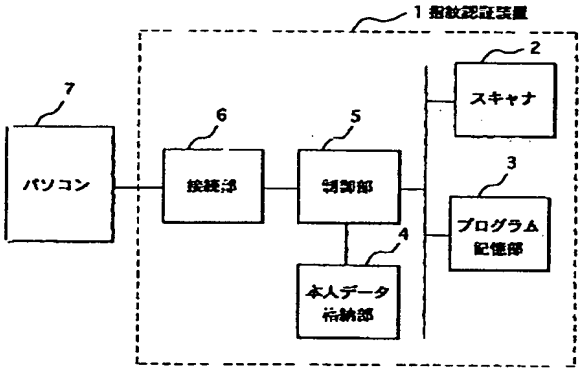
【図１】図１は、本発明に係るシステムの構成を示すブロック図である。

【図2】図2は、図1に示すパソコン7の構成を示すブロック図である。
【図3】図3は、図1に示すシステムの動作を説明するフローチャートである。
【図4】図4は、図1に示すパソコン7のメモリ23のメモリ空間を説明する図である。
【図5】図5は、従来の指紋認証装置の構成を示すブロック図である。

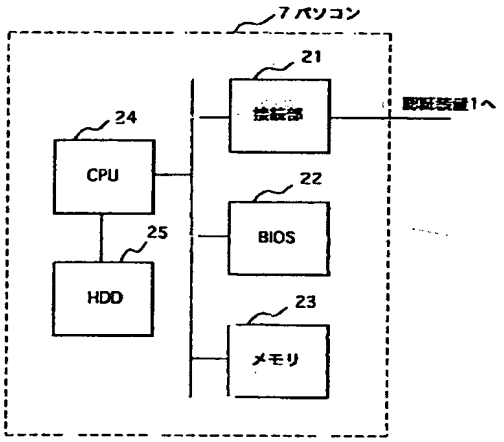
【符号の説明】

1	指紋認証装置
2	スキャナ
3	プログラム格納部
4	本人データ格納部
5	制御部
6	接続部
7	パソコン

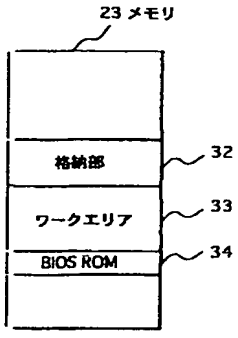
【図1】



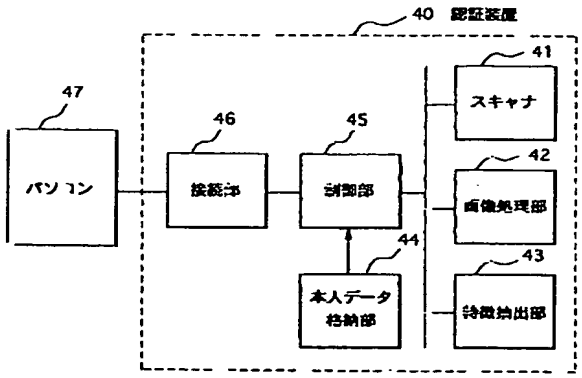
【図2】



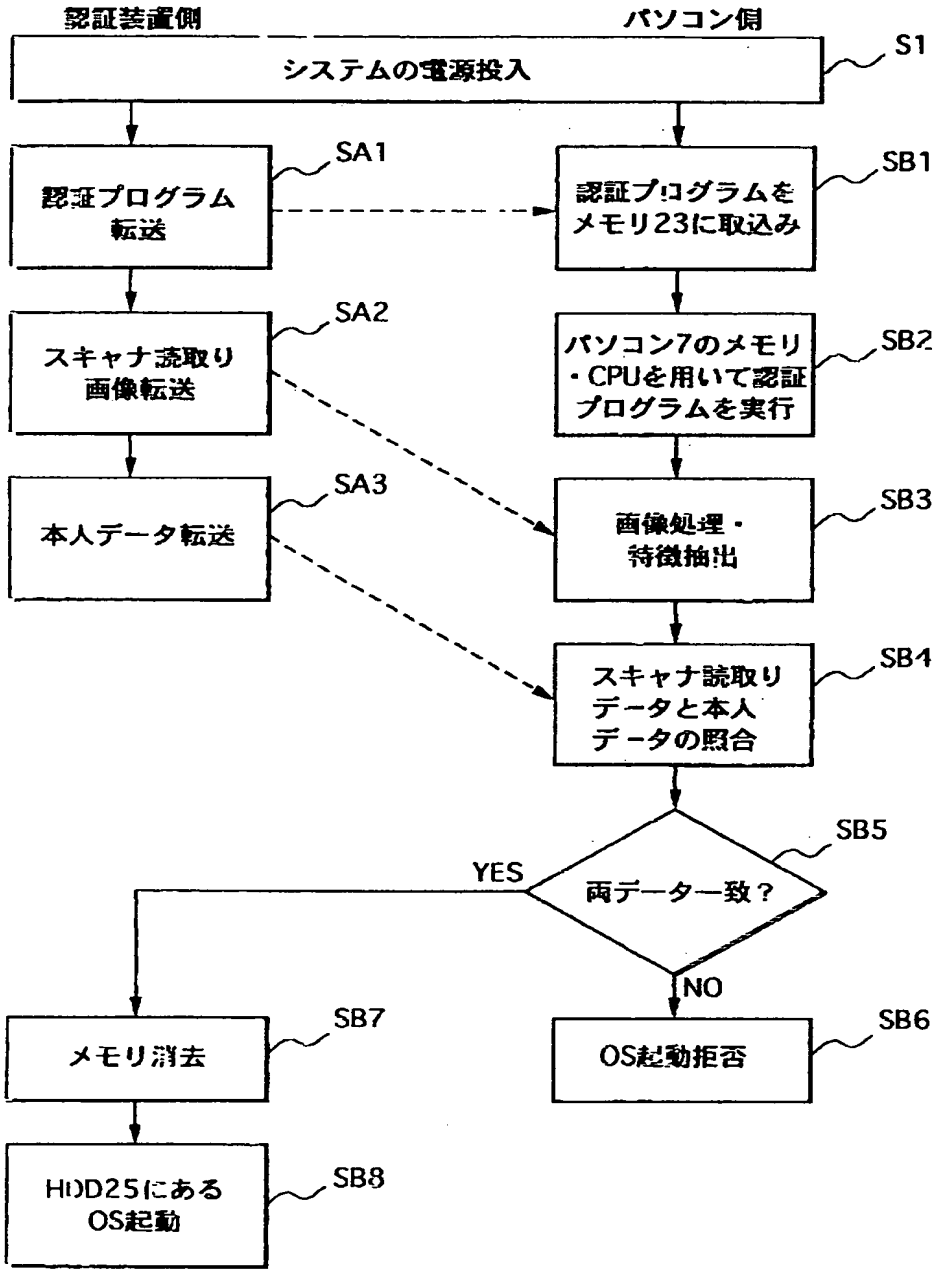
【図4】



【図5】



【図3】


認証装置側
パソコン側
システムの電源投入
S1
認証プログラム転送
SA1
認証プログラムをメモリ23に取込み
SB1
スキャナ読取り画像転送
SA2
パソコン7のメモリ・CPUを用いて認証プログラムを実行
SB2
本人データ転送
SA3
画像処理・特徴抽出
SB3
スキャナ読取りデータと本人データの照合
SB4
両データ一致？
SB5
YES
NO
メモリ消去
SB7
OS起動拒否
SB6
HDD25にあるOS起動
SB8